BY ORDER OF THE
SECRETARY OF THE AIR FORCE

AIR FORCE INSTRUCTION 33-207

1 SEPTEMBER 1997

Communications and Information

COMPUTER SECURITY ASSISTANCE PROGRAM

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

NOTICE: This publication is available digitally on the SAF/AAD WWW site at: http://afpubs.hq.af.mil. If you lack access, contact your Publishing Distribution Office (PDO).

OPR: HQ AFCA/SYS
(CMSgt Hogan)

Certified by: HQ USAF/SCXX
(Lt Col Francis X. McGovern)
Pages: 5
Distribution: F

This instruction implements Air Force Policy Directive (AFPD) 33-2, *Information Protection*, establishes the Air Force Computer Security Assistance Program (CSAP) and identifies responsibilities. It applies to all Air Force organizations. Refer recommended changes and conflicts between this and other publications on AF Form 847, **Recommendation for Change of Publication,** through channels, to HQ Air Force Communications Agency (HQ/XPPD), 203 W Losey Street, Room 1065, Scott AFB IL 62225-5224, with an information copy to AFIWC/EA, 250 Hall Blvd, Ste 139, San Antonio TX, 78243-7063; HQ Air Force Communications and Information Center (HQ AFCIC/SYNI, 1250 Air Force Pentagon, Washington DC 20330-1250; and HQ AFCA/SYS, 203 W Losey St, Rm 2040, Scott AFB IL, 62225-5234. **Attachment 1** lists references, abbreviations, acronyms, and terms used in this instruction.

1. Purpose. This instruction establishes the CSAP and lists responsibilities for applicable organizations. The CSAP supports the Air Force Information Protection Program outlined in AFPD 33-2.

2. Responsibilities.

2.1. HQ Air Force Communications and Information Center (HQ AFCIC/SY NI) directs the Air Force Information Protection (IP) program.

2.2. Air Force Information Warfare Center (AFIWC) will:

2.2.1. Manage the CSAP to support the Air Force IP program, and MAJCOM Information Protection Assessment and Assistance Program (IPAP) (AFI 33-230, *Information Protection Assessment and Assistance Program*.)

2.2.2. Serves as the Air Force focal point for IP operations and support organizations conducting them. (AFI 33-208, *Information Protection Operations*.)

2.2.3. Provide IP guidance to Air Force developers of information, sensor, and weapon systems.

2.2.4. Manage the Air Force Computer Emergency Response Team (AFCERT) program.

2.2.5. Serve as the Air Force single point of contact for reporting and handling computer security incidents and vulnerabilities including AFCERT advisories and Defense Information Systems Agency (DISA) automated systems security incident support team (ASSIST) bulletins.

2.2.6. Using computer security engineering teams (CSET**),** provide on-site incident response assistance to information systems users and organizations to assess, control, and recover from actual intrusion activity. When requested, CSETs, provide on-site technical assistance and recommendations to computer users and organizations on computer and computer network security matters and support MAJCOM IPAPs according to AFI 33-230.

2.2.7. Coordinate the technical resources of AFIWC to identify (and/or develop), analyze, and publicize the availability of countermeasures for reported computer and computer network security incidents and vulnerabilities.

2.2.8. Maintain a CSAP Database System (CDS). The database will consist of detailed information concerning hardware, software, information systems and network mapping (NMAP), system connectivity, vulnerabilities, malicious logic proliferation, countermeasures, and “hacker” techniques. Provide CDS access to Air Force Network Control Centers (AFNCC), Information Warfare Squadrons (IWS), and wing and MAJCOM IP offices.

2.2.9. Collect and evaluate intrusion detection data. Report suspicious activities to MAJCOM and wing IP offices for deconfliction. Resolve all validated unauthorized activity, consulting with MAJCOM/FOA/wing IP personnel, as necessary. Provide annual summaries to MAJCOM/FOA IP offices and HQ AFCA/SYS.

2.2.10. Analyze automated information systems (AIS) vulnerabilities data and provide to HQ AFCA/SYS for metric and assessment purposes according to AFPD 33-2 and AFI 33-205*, Information Protection Metrics and Measurements.*

2.2.11. Perform statistical, threat, and threat posture analysis, and distribute as required.

2.2.12. Identify operational countermeasures for vulnerabilities and publicize their availability (in the CSAP Database System) to MAJCOM/FOA IP offices.

2.2.13. Identify requirements for IP tools and provide guidance on the use of these tools to Air Force organizations.

2.2.14. Develop and analyze threat information and provide an annual threat assessment report to appropriate organizations.

2.2.15. Conduct IP operations according to AFI 33-208. ***NOTE:*** The reporting requirements in paragraphs **2.2.9.**, **2.2.10.**, **2.2.11.**, and **2.2.14.** are exempt from licensing according to AFI 37-124, *The Information Collection and Reports Management Program; Controlling Internal, Public, and Interagency Air Force Information Collections* (will convert to AFI 33-324.)

2.3. MAJCOM IP offices will submit requests for CSET support to AFIWC/EA.

2.4. Wing IP offices will submit requests for CSET support to their MAJCOM IP office.

2.5. HQ AFCA/SYS will use CSAP data to meet assessment and metrics requirements reporting according to AFPD 33-2 and AFI 33-205.

WILLIAM J. DONAHUE, Lt General, USAF
Director, Communications and Information

Attachment 1

GLOSSARY OF REFERENCES, ABBREVIATIONS, ACRONYMS, AND TERMS

References

AFPD 33-2, *Information Protection*

AFI 33-205, *Information Protection Metrics and Measurements*

AFI 33-208, *Information Protection Operations*

AFI 33-230, *Information Protection Assessment and Assistance Program*

Abbreviations and Acronyms

AFCA—Air Force Communications Agency

AFCERT—Air Force Computer Emergency Response Team

AFCIC—Air Force Communications and Information Center

AFI—Air Force Instruction

AFIWC—Air Force Information Warfare Center

AFNCC—Air Force Network Control Center

AIS—Automated Information System

ASIM—Automated Security Incident Measure

AFNCC—Air Force Network Control Center

CDS—CSAP Database System

CSAP—Computer Security Assistance Program

CSET—Computer Security Engineering Team

DISA—Defense Information Systems Agency

DRU—Direct Reporting Unit

FOA—Field Operating Agency

IP—Information Protection

IPAP—Information Protection Assessment and Assistance Program

IWS—Information Warfare Squadron

MAJCOM—Major Command

Terms

Automated Information Systems (AIS)—1. Any equipment or interconnected system or subsystems of equipment that is in the automated acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data and includes computer software, firmware, and hardware. ***NOTE:*** Included are computers, word processing systems, networks, or other electronic information handling systems, and associated equipment. 2. A combination of information, computer, and telecommunications resources and other information technology and personnel resources that collect, record, process, store, communicate, retrieve, and display information (Air Force Directory 33-121.)

Computer Security Engineering Team (CSET)—Deployable teams that provide assistance to computer users and Air Force organizations. CSETs also provide assistance to control and recover from intrusion activity.

Information Protection (IP)—Measures to protect friendly information systems by preserving the availability, integrity, and confidentiality of the systems and the information contained within the systems. See AFPD 33-2.

Information Protection Assessment Program (IPAP)—A MAJCOM function established to assess the effectiveness of wing IP programs and provide assistance when necessary.

Information Protection Operations—Proactive security functions established to assist Air Force organizations to deter, detect, isolate, contain, and recover, from intrusions of computers and computer networks.

Information Protection Solutions—Tools, processes, training, personnel, policy, and procedures which achieve the desired level of information protection.

Information Protection Tools—IP tools perform numerous security functions including boundary protection, viral detection, intrusion detection, configuration inspection, network mapping, remote patching, and on-line surveys determining status of vulnerabilities, etc**.**

Network Mapping (NMAP)—Detailed information on specific computers and computer networks consisting of hardware, installed software, operational system description, criticality and sensitivity of the data processed, accreditation status and date, location, internet protocol address, and system administrator points of contact. NMAP is used for network management and network security.

Suspicious Activity—Suspicious activity includes failed log-ins, changes to privileges, and renamed user account/privileges.